ITU Zombie Botnet Mitigation Project: Background & Approach

17 October 2007

Robert Shaw & Suresh Ramasubramanian
<cybmail@itu.int>

ICT Applications and Cybersecurity Division
Policies and Strategies Department, BDT
International Telecommunication Union

Botnets – An Overview

- What is a Botnet?
  - ➢ A collection of infected and compromised computing devices, harnessed together and remotely controlled for malicious purposes

- How powerful is a Botnet?
  - ➢ Supercomputers
  - ➢ Distributed Computing Systems
    - BOINC – Used for SETI@Home, Atomic Physics
    - People agree to donate spare computing resources
  - ➢ Botnets: A special case of Distributed Computing
    - Without the consent of the computers' owners
    - More computing power than a supercomputer – for free

The Botnet Economy

- Virus Writers, Botherders, Clients
  - ➢ Virus writer writes malware, infects computers to create a botnet
  - ➢ Botherder operates the botnet's "command and control" (C&C)
  - ➢ Clients hire botnets to use for Spam, DDoS, Identity Theft
- Highly developed underground economy
  - ➢ Underground channels of communication
    - ▪ "Secret" forums and chat rooms that frequently shift location
    - ▪ Access shared on a need to know basis, new entrants may need to be vouched for by an existing participant
  - ➢ Botherders offer support contracts to clients
    - ▪ Guaranteed replacement of botnet in case antivirus researchers release a fix for the malware, or the botnet is taken down
- Organized crime involved in all stages of the economy
  - ➢ Employ virus writers to create malware
  - ➢ Carry out spam campaigns, espionage, ID theft, cyber attacks
  - ➢ Launder money stolen from victims

Evolution of Botnets

- C&C centers harder to trace
  - Originally hosted on public IRC channels
  - Now encrypted, access restricted C&C software
- C&C centers may be hosted on botnets
  - Increased redundancy
  - Makes takedown harder
- New "headless" single use botnets
  - No centralized control or C&C required
  - Instructions embedded into the malware
  - New malware and botnet created for a new task
  - Cannot stop botnet by taking down its C&C

Evolution of Malware

- Malware is Self Propagating
  - ➢ Infected hosts infect other hosts
    - Infection vectors include email, P2P networks, open shared network folders, visiting an infected website
    - Newer malware spreads faster than older generations of malware
  - ➢ Its spread resembles that of a global pandemic (SARS, Bird Flu)
    - Similar threat models and mitigation mechanisms can be applied
- Malware is becoming increasingly sophisticated
  - ➢ Earlier, mostly spread through infected floppy disks
  - ➢ Spreads much faster over the internet
    - Email, IM, compromised websites, P2P, network shared folders)
  - ➢ Principles of software engineering evident in recent malware
  - ➢ Analysis, Detection and Removal more difficult
    - Self destruct mechanisms to destroy data if the malware is removed
    - "Droppers" download more malware onto a compromised host
    - Encryption and Debugger / VM traps to prevent forensic analysis

What can you do with a Botnet?

- Spam
  - ➤ The most visible use of botnets
  - ➤ Botnets can host an entire spam campaign
    - DNS servers, website hosting, spam sending
    - Content can change location from PC to PC, country to country, in minutes
  - ➤ "Take" from a spam run can be reused
    - 419 scam artists now buying lists of compromised accounts from botherders, using these to spam
  - ➤ Spam is just the tip of the iceberg.

What else can you do with a botnet?

- Attack a country's Internet infrastructure
  - ➢ Estonia – 128 unique DDoS attacks in two weeks
- Extortion
  - ➢ Threaten to DDoS and cripple ecommerce websites
- Identity theft and Industrial Espionage
  - ➢ Steal credit cards, passwords etc from infected PCs
  - ➢ Use the computing power of a botnet to break into secured networks and steal data, credit cards
- Stock "Pump and Dump" scams
  - ➢ Use spam from botnet PCs to advertise a stock
  - ➢ Trade in this stock using online share trading accounts from infected PCs, artificially boost prices

International
Telecommunication
Union

Australian Internet Security Initiative

- Watch, Warning & Incident Response System
  - ➢ Public Private Partnership
- ACMA, together with 25 Australian ISPs
  - ➢ ACMA collects data about IPs emitting malware
    - Identifies IPs operated by participating Australian ISPs
    - Notifies the ISP responsible for affected IPs
  - ➢ The ISP undertakes to mitigate malware activity from the affected IPs on their networks
    - Notify infected customers
    - Change security and filtering policies as necessary
- AISI to be shared with international partners
  - ➢ Proposed strategic cooperation between ITU and ACMA
  - ➢ Extend AISI to ITU member states

Botnet Mitigation Package

- Broadly parallels previous efforts such as the OECD Spam Toolkit
- Identify nodal agency for a nationwide botnet mitigation strategy
  - ➢ Multistakeholder, Multipronged Approach
  - ➢ Public Private Partnership
  - ➢ Make best possible use of existing initiatives and structures
- Infrastructure for botnet scanning, measurement and mitigation
  - ➢ Capacity building on tools and techniques to track botnets
  - ➢ Identification of trusted reporters (international security and AV research community, CERT teams et al) for incident reporting
- Detection and Takedown of botnet hosts and infrastructure
  - ➢ Infected PCs (automate as far as possible), C&C hosts, domains registered for a botnet, payment gateways used by botnets etc
- Awareness of security best practices for ISPs, ecommerce sites
- Ensure public access to secure ICT, awareness of Internet safety
  - ➢ Engage local civil society for assistance and grassroots penetration
- Framework for botnet related policy, regulation and enforcement;
- Multistakeholder international cooperation and outreach
  - ➢ COE Cybercrime Convention, LAP, APECTEL/OECD, MAAWG, APWG

Current Shortcomings – Policy

- Lack of relevant Cybercrime and antispam legislation
  - ➤ Existing Cybercrime / spam laws may need to be updated or revised, keeping botnet related crime in mind
- Capacity building for regulators, police, judiciary
  - ➤ Training existing officials may be supplemented by co-opting or active recruitment of technical experts
- Paucity of international cooperation and outreach
  - ➤ Participation in local, regional and international initiatives
  - ➤ Engagement of relevant government, regulators, law enforcement with their peers and other stakeholders around the world
  - ➤ Active outreach to countries and stakeholders known to be particularly susceptible to Cybercrime issues

Shortcomings: Industry, Public

- ISPs, eCommerce vendors require capacity building
  - Engagement with international industry groups
  - Promotion of industry wide security best current practices
    - Antispam, Anti Malware, Credit Card Fraud, Network Security
  - Suggested re-engineering of security policies
- Education and access to secure ICT for users
  - Awareness of common scams
  - Availability and use of Firewalls, Antivirus Software
  - Motivation to avoid the use of pirated software
- Paucity of cooperation and public private partnerships
  - Participation at grassroots, national and international levels
    - Participation has to be relevant, meaningful and informed.
    - Capacity building [and funding] for relevant stakeholders to ensure meaningful participation in local, regional and international initiatives
    - Bridge the information and perception gaps between stakeholders

October 2007

11

Proposed Project Activities

- Measures for botnet detection, measurement and mitigation
  - ➤ Identify existing initiatives, best practices and stakeholders
    - Adapt existing best practices to suit local conditions, as necessary
  - ➤ Build watch, warning and incident response systems
    - AISI, alerts from CERT and security research groups et al
  - ➤ Maintain open and public channels of communication
  - ➤ Integrate botnet mitigation with general ICT development
    - Pandemic treatment and mitigation vis a vis public health initiatives
    - Holistic approach required to improve the general "Internet Health"

- Field mission to help extend AISI and other relevant measures to a developing economy [as a pilot project]

- Draft, in association with AISI, the national framework for botnets mitigation, part 2 of the package

Proposed activities (continued)

- Organize workshop for botnets mitigation
  - ➢ Bring representatives of existing initiatives and relevant experts together with other stakeholders
  - ➢ Promote and facilitate capacity building
- Identify and share existing sources of information
  - ➢ Make relevant best practice documents widely available
  - ➢ Translate these into the official UN languages
  - ➢ Encourage contribution of translations in other languages
- Finalize the botnets mitigation package
  - ➢ Translate and widely disseminate
- Proposed annual forum on botnet mitigation
  - ➢ Integrate with current WSIS C5 activities, thematic meets
  - ➢ Possible cooperation with an existing international forum